УДК 004.056.55

В.Б. Уфимцева, Н.Ю. Карпенко

Харьковский национальный университет городского хозяйства им. А.Н. Бекетова

АНАЛИЗ ПОКАЗАТЕЛЕЙ ПЕРЕМЕШИВАНИЯ В СЕТЯХ ФЕЙСТЕЛЯ

В статье сосредоточено внимание на исследовании процедур перестановок в симметричных шифрах со структурой сети Фейстеля (СФ) с целью улучшения показателей перемешивания по Шеннону. А именно, на возможностях улучшения показателей перемешивания при использовании в перестановке нескольких циклов и операций сложения в фактор-кольце $Z/(q)$. Проведен анализ наиболее подходящей с точки зрения диффузионного процесса структуры – схемы Фейстеля и исследована целесообразность использование в схеме обмена (СО) симметричного шифра циклических операций сложения.

***Ключевые слова**: симметричное шифрование, сети Фейстеля, схема обмена, диффузия.*

Постановка проблемы и анализ последних исследований

При разработке симметричных блочных шифров широкую популярность приобрела криптосистема, названная схемой Фейстеля. Впервые она была использована Хорстом Фейстелем в 1973 г. при разработке шифра Lucifer [1], и затем применялась во многих разработках блочных шифров, в том числе и в финалистах AES [2] (TWOFISH, MARS и RC6).

Схема Фейстеля (СФ) является методом смешивания подблоков входного текста в шифре посредством повторяющегося применения зависящих от ключей нелинейных функций, называемых F-функциями (рис. 1) и выполнения перестановок подблоков.

Раунд блокового шифра является преобразованием, которое соединяет подблоки входного блока посредством F-функций и перестановок подблоков.

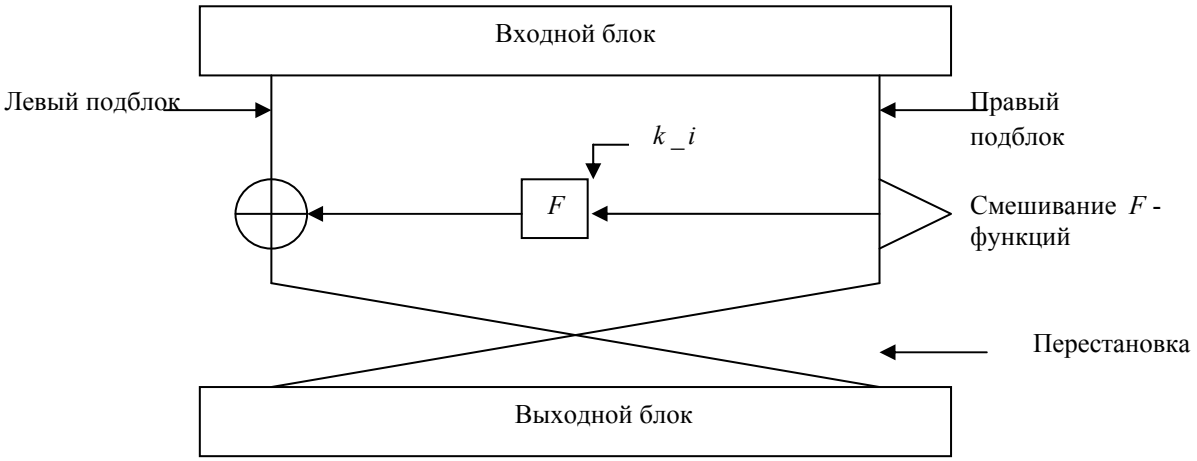


Рис. 1. Стандартная схема Фейстеля

В стандартной СФ открытый текст разбивается на два полублока одинаковой длительности. Обобщенная СФ может разбивать входной блок на $n \geq 2$ подблоков. Далее подразумевается, что все подблоки имеют одинаковую длину, так что каждый подблок может участвовать в транспозиции с любым другим подблоком. Обобщенная схема обмена (СО) является перестановкой $n \geq 2$ подблоков в раунде.

Необходимым условием стойкости шифра является достижение полной диффузии. Диффузионный процесс шифра (функции) характеризуется результатом распространения влияние одного входного бита на много выходных. Шифр (функция) называется полным, если каждый выходной бит зависит от всех входных [3]. В последующем анализе все F-функции подразумеваются полными.

Важную роль в процессе диффузии в блочных шифрах играют схемы смешивания. Подходящая связь между смесью F-функции и СО существенно улучшает процесс диффузии, т.е. увеличивается быстродействие метода, вследствие чего можно уменьшить количество итераций в алгоритме, построенном на основе этого метода. Отдельно они могут не достигать свойства полной диффузии. Полная диффузия в схеме, с точки зрения влияния всех подблоков входа на все подблоки выхода, достигается после того, как все подблоки были на входе одной определенной F-функции, и после того, как каждому подблоку на выходе F-функции будет предшествовать цепочка из комбинации всех подблоков.

Среди AES кандидатов [2], базирующихся на схеме Фейстеля, структуры процессов Twofish, Mars и RC6 наиболее быстро достигают полной диффузии с точки зрения влияния всех подблоков входа на все подблоки выхода. Twofish достигает полной диффузии после трех $(2, 2)$ F-функций (раундов) и Mars – после пяти $(1, 3)$ F-функций (раундов) [4].

Финалист конкурса на звание стандарта шифрования AES шифр RC6 является схемой Фейстеля с четырьмя подблоками и двумя $(2, 1)$ F-функциями в раунде (рис. 2), то есть два подблока преобразуются функцией от ключа и других двух подблоков. Период P однокластерной схемы обмена шифра RC6 равен количеству подблоков, то есть $P = 4$. Полная диффузия достигается после трех раундов, как видно из прямой схемы диффузии на рис. 2.

Диффузионный процесс неодинаково влияет на подблоки шифра RC6, что видно из зависимостей выходов нелинейных F-функций от входных подблоков (A_0, B_0, C_0, D_0):

$$
\begin{aligned}
&A_1 = A_2 = A_0 \oplus F\_k_1(B_0, D_0)\\
&B_1 = B_0\\
&C_1 = C_2 = C_0 \oplus F\_k_2(B_0, D_0)\\
&D_1 = D_0\\
&B_3 = B_2 =\\
&= B_0 \oplus F\_k_4(A_0 \oplus F\_k_1(\ ), C_0 \oplus F\_k_2(\ ))\\
&D_3 = D_2 =\\
&= D_0 \oplus F\_k_3(A_0 \oplus F\_k_1(\ ), C_0 \oplus F\_k_2(\ ))\\
&A_3 = F\_k_6(D_0 \oplus F\_k_3(\ ), B_0 \oplus F\_k_4(\ ))\\
&C_3 = F\_k_5(D_0 \oplus F\_k_3(\ ), B_0 \oplus F\_k_4(\ )).
\end{aligned}
\qquad (1)
$$

Из зависимостей (1) видно, что после двух раундов полной диффузии достигают только два подблока (B и D), два других подблока (A и C) достигают полной диффузии после трех раундов (табл. 1).

Таким образом, диффузионный анализ шифра RC6 показал, что для достижения полной диффузии в RC6 требуется вычисление шести $(2, 1)$ F-функций.

В работе [5] была исследована целесообразность использование в СО умножения на обобщенную матрицу Фибоначчи.

Была рассмотрена схема Фейстеля с цепочечной схемой смешивания (2, 1) F-функций и схемой обмена на основе умножения на Q_p^n-матрицу Фибоначчи в фактор-кольце $Z/(q)$ при различных значениях порядка p и степени n матрицы.

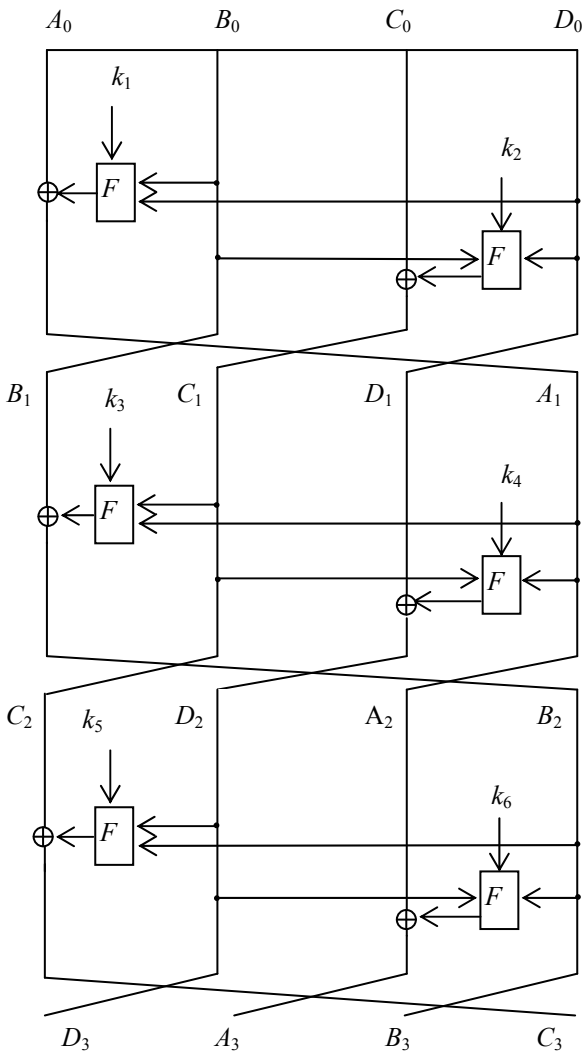
Схема процедуры матричного преобразования Фибоначчи (МПФ) в СО использует умножение (p+1)x(p+1)-матрицы данных, состоящей из подблоков, на Q_p^n -матрицу Фибоначчи в фактор-кольце $Z/(q)$ сводится к операциям сложения и сдвига подблоков.

В схеме МПФ производится N вычислений F-функции для N подблоков в каждом раунде. При такой схеме смешивания (2, 1)-F -функций первый раунд делает три последних подблока полными, следующий раунд делает все подблоки полными. Следовательно, достаточно только двух раундов для полной диффузии.

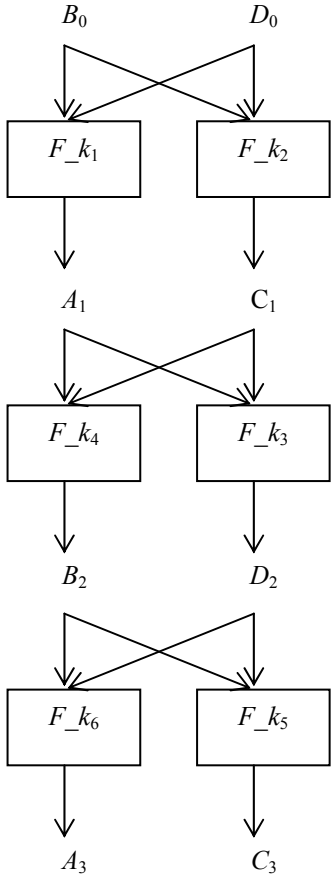
Таблица 1

Распространение диффузии в RC6

подблоки / раунды	A	B	C	D
1	A, B, D	B	B, C, D	D
2	A, B, D	A, B, C, D	B, C, D	A, B, C, D
3	A, B, C, D	A, B, C, D	A, B, C, D	A, B, C, D



а)



б)

Рис. 2 . Схема диффузии первых раундов RC6:
а) схема шифра;
б) прямая схема диффузии

При порядке матрицы Фибоначчи p=1 и степенях n=±1 и n=±2 (рис. 3 и рис. 4) входной блок разбивается на четыре подблока, как и в RC6, а схема обмена состоит из двух кластеров по два подблока. Один раунд равен двойному раунду RC6, так как содержит четыре F-функции. В зависимости от степени матрицы Фибоначчи выходными подблоками являются подблоки соответствующей степени (A^n, B^n, C^n, D^n), т.е. для n>0 (рис. 3):

$$
\begin{aligned}
A_1^1 &= A_0 \oplus F\_k_1(B_0, D_0)\\
A_1^2 &= 2\cdot F\_k_1(\,) + F\_k_2(F\_k_1(\,), C_0)\\
B_1^2 &= B_1^1 = F\_k_1(\,) + F\_k_2(F\_k_1(\,), C_0).\\
C_1^1 &= F\_k_3(F\_k_2(\,), D_0)\\
C_1^2 &= 2\cdot F\_k_3(\,) + F\_k_4(F\_k_3(\,), F\_k_1(\,))\\
D_1^2 &= D_1^1 = F\_k_3(\,) + F\_k_4((\,), F\_k_1(\,))
\end{aligned}
\qquad (2)
$$

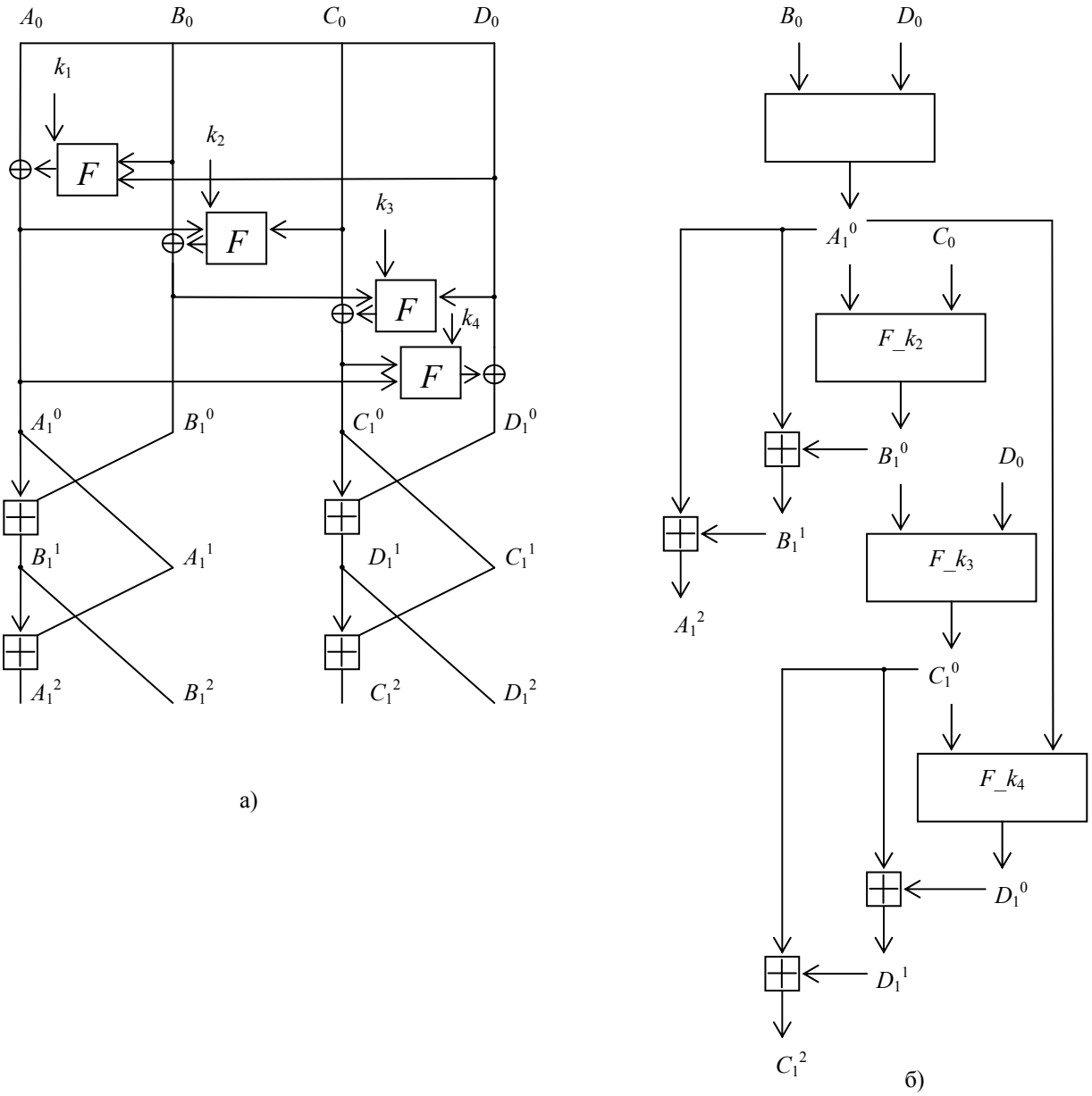


Рис. 3. Схема диффузии МПФ при $p = 1$ и $n = 1$ и n = 2:
а) схема шифра;
б) прямая схема диффузии

Зависимости выходных подблоков от входных при степени матрицы Фибоначчи $n < 0$ (рис. 4) принимают вид (3).

Из зависимостей (2) видно, что при n=1 за один раунд (после вычисления четырех F-функций) полной диффузии достигают три подблока (B, C, D), что лучше, чем в RC6, где после вычисления четырех F-функций полной диффузии достигают только два подблока (табл.2).

$$
\begin{aligned}
A_1^{-2} &= A_1^{-1} = F\_k_1(A_0, B_0, D_0) - F\_k_2(F\_k_1(\ ), C_0) \\
B_1^{-1} &= F\_k_2(F\_k_1(A_0, B_0, D_0), C_0) \\
B_1^{-2} &= 2 \cdot F\_k_2(F\_k_1(\ ), C_0) - F\_k_1(\ ) \\
C_1^{-2} &= C_1^{-1} = F\_k_3(F\_k_2(\ ), D_0) - \\
&- F\_k_4(F\_k_3(\ ), F\_k_1(\ )) \\
D_1^{-1} &= F\_k_4(F\_k_3(\ ), F\_k_1(\ )) \\
D_1^{-2} &= 2 \cdot F\_k_4(F\_k_3(\ ), F\_k_1(\ )) - F\_k_3(\ )
\end{aligned}
\qquad (3)
$$

Во втором раунде выполнение двух F-функций делает подблок F полным, т. е. для достижения полной диффузии МПФ требуется выполнение шести F-функций (аналогично RC6). Однако, при n=2, n=–1 и n=–2, как видно из зависимостей (2) и (3), все подблоки достигают полной диффузии за один раунд. Т. е. для достижения полной диффузии МПФ требуется выполнение четырех F-функций, что меньше, чем в RC6 и в СФ с аналогичной схемой смешивания F-функций.

Таким образом, шифр МПФ при p=1 и трех значениях степени матрицы Фибоначчи из четырех достигает полной диффузии быстрее, чем RC6 и СФ с аналогичной схемой смешивания F-функций (табл.2).

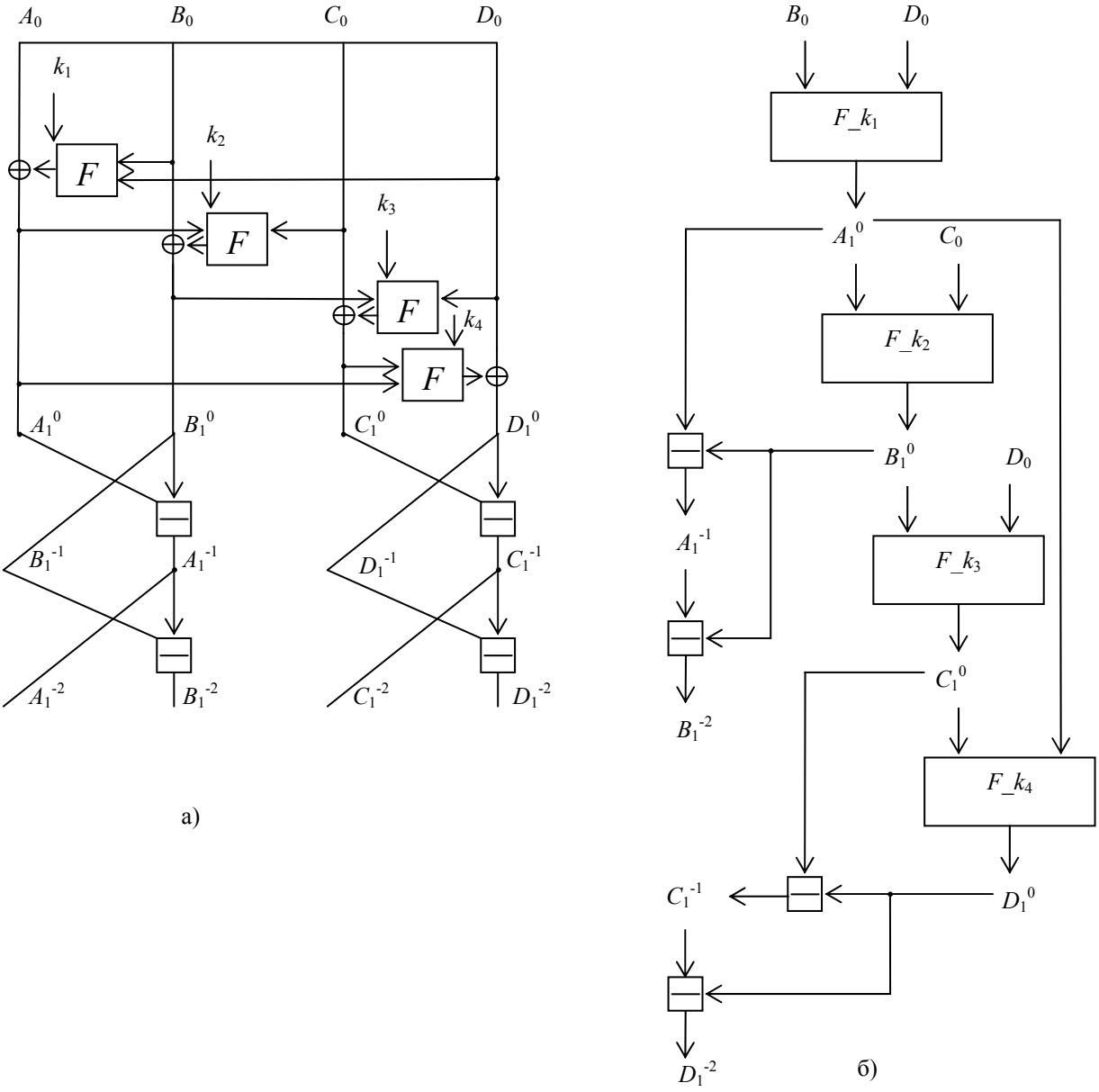


Рис. 4. Схема диффузии МПФ при p = 1 и n = –1 и n = –2:
а) схема шифра;
б) прямая схема диффузии

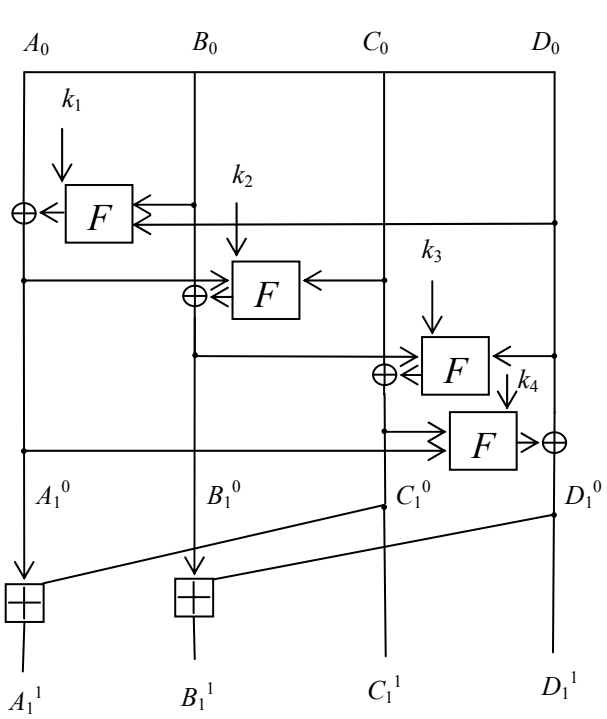
Таблица 2

Распространение диффузии в МПФ с четырьмя подблоками при степени матрицы Фибоначчи $n = -2 \div 2$

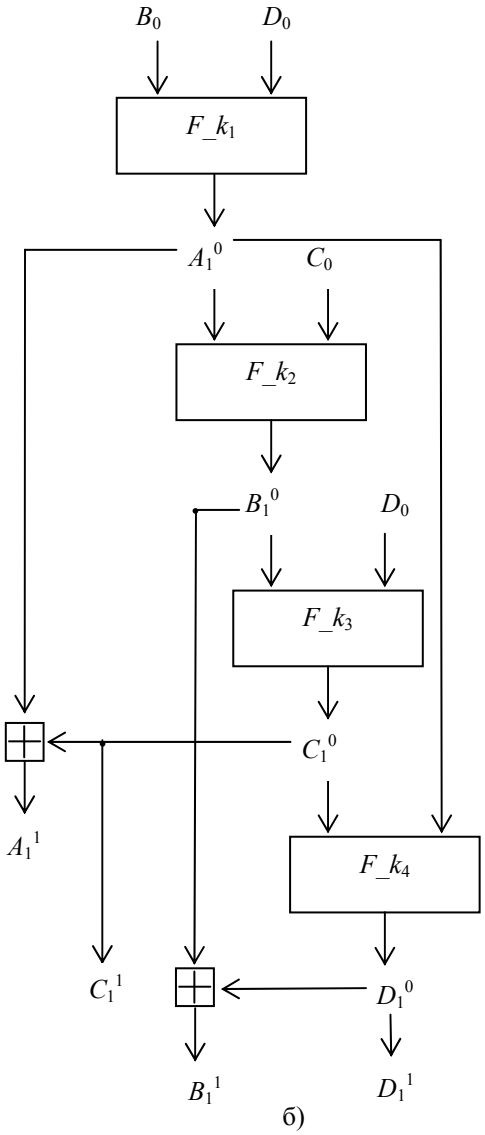
раунд	подблоки / n	A	B	C	D
1	1	A, B, D	A, B, C, D	A, B, C, D	A, B, C, D
	2	A, B, C, D	A, B, C, D	A, B, C, D	A, B, C, D
	-1	A, B, C, D	A, B, C, D	A, B, C, D	A, B, C, D
	-2	A, B, C, D	A, B, C, D	A, B, C, D	A, B, C, D
2	1	A, B, C, D	A, B, C, D	A, B, C, D	A, B, C, D

В работе [5] было доказано усиление диффузии при использовании в схеме обмена СФ умножения на матрицу Фибоначчи. Однако, принимая во внимание, что данная операция умножения сводится к сложению и сдвига подблоков, то **целью исследования** является рассмотрение использования операции сложения в других схемах обмена.

Исследование. Основным недостатком МПФ видится использование кластеров в СО, что влечет невозможность достижения полной диффузии за 1 раунд с одним циклом сложения и сдвига. В [4] были показаны преимущества СО без кластеров, перемешивающих все подблоки входного текста. Проанализировав ряд вариантов преобразований шифра МПФ, получили шифр Add (рис. 5).



а)



б)

Рис. 3.5. Схема диффузии шифра Add :
а) схема шифра;
б) прямая схема диффузии

Зависимости выходных подблоков от входных шифра Add принимают вид:

$$\begin{aligned} A_1^1 &= A_0 \oplus F\_k_1(B_0, D_0) + C_0 \oplus F\_k_3(\ ) \\ B_1^1 &= B_0 \oplus F\_k_2(F\_k_1(\ ), C_0) + D_0 \oplus F\_k_4(\ ) \\ C_1^1 &= C_0 \oplus F\_k_3(F\_k_2(\ ), D_0) \\ D_1^1 &= D_0 \oplus F\_k_4(F\_k_3(\ ), C_0) \end{aligned} \quad (4)$$

Как видно из зависимостей (4), применение операции сложения к первым подблокам позволило получить распространение влияния каждого подблока на каждый. То есть при использовании такой схемы обмена полная диффузия достигается, в отличии от схемы МПФ, за один раунд во всех подблоках (табл. 3).

Критерием диффузионного процесса на практике является строгий лавинный критерий (СЛК) и критерий распространения степени *m*.

Булева функция удовлетворяет СЛК, если любой выходной бит изменяется с вероятностью строго ½ при комплементарной замене одного входного бита:

$$(\forall a : W_H(a) = 1) \quad P(f(X) = f(X \oplus a)) = 1/2 . \quad (5)$$

Проверка на удовлетворение криптографической функции МПФ строгому лавинному критерию была проведена путем формирования двух комплементарных входов, сложения полученных выходов в $GF(2)$ и проверке полученной битовой последовательности по статистическому тесту проверки равномерности (частот) – Frequency (Monobit) Test Американского института стандартов NIST для криптографических функций [6].

«NIST Statistical Test Suite» – статистический пакет, состоящий из 16 тестов, разработанных для проверки случайности двоичных последовательностей, производимых или техническими средствами, или программным обеспечением.

Цель The Frequency (Monobit) Test (Частотный (монобитный) тест) состоит в определении того, является ли число единиц и нулей в последовательности таким, каким может ожидаться для случайной последовательности.

Тесты показали, что для шифра с исследуемой схемой обмена количество раундов, требуемых для удовлетворения СЛК, меньше, чем у шифра МПФ.

Расширением понятия СЛК является критерий распространения степени *m*.

Булева функция удовлетворяет критерию распространения степени *m* в том случае, если комплементация *m* или менее входных координат приводит к комплементации выхода в 50% случаев при всех возможных входных векторах. Строгий лавинный критерий является критерию распространения степени 1.

Проверка проводилась аналогично проверке на СЛК с комплементацией m=2÷126 входных координат, сложением полученных выходов в GF(2) и проверкой полученной битовой последовательности по статистическому тесту проверки равномерности (частот) [77] – Frequency (Monobit) Test. Тестирование проводилось при фиксированных ключе, длина входного блока составляла 4*32=128 бит. Тестировалось 10000 последовательностей более 10240 бит в каждой.

Результаты тестов показали удовлетворение Add с четырьмя подблоками и длиной входа 128 бит критерию распространения максимальной степени *m* = 126, что говорит о высокой степени нелинейности шифра.

Результаты статистического анализа критериев сбалансированности, корреляции между входом и выходом алгоритма и корреляционного иммунитета подтвердили сохранении статистической стойкости шифра.

Таким образом, статистические исследования строгого лавинного критерия подтвердили повышение скорости диффузии по сравнению с аналогом, шифром МПФ, благодаря использованию цикличной операции сложения.

Таблица 3

Распространение диффузии в Add

подблоки / раунды	A	B	C	D
1	A, B, C, D	A, B, C, D	A, B, C, D	A, B, C, D

Вывод

В статье проанализированы варианты реализации симметричного шифра на основе модифицированной схемы Фейстеля с использованием в схеме обмена операции сложения.

В результате проведенного анализа наиболее подходящей с точки зрения диффузионного процесса структуры СФ была выбрана схема обмена с использованием операции сложения таким образом, чтобы достижение полной диффузии происходило за первый цикл.

Анализ показал, что шифр Add с такой схемой достигает полной диффузии в 1,5 раза быстрее, чем финалист AES шифр RC6 и в 2 раза быстрее СФ с аналогичной схемой смешивания F-функций и быстрее шифра МПФ.

Статистические исследования строгого лавинного критерия подтвердили повышение скорости диффузии по сравнению с аналогами – шифром RC6 и МПФ благодаря использованию в схемы обмена безкластерной операции сложения. Add удовлетворяет СЛК после 2 раундов, что аналогично четырем раундам RC6, а последний – только после пяти раундов.

Результаты статистического анализа критериев сбалансированности, корреляции между входом и выходом алгоритма и корреляционного иммунитета подтвердили сохранении статистической стойкости метода. Выходная последовательность Add имеет свойства случайной после 1 раунда (2 раунда RC6), что на 2 раунда быстрее, чем у метода RC6.

Таким образом, увеличение скорости процесса диффузии усиливает криптостойкость алгоритмов и позволяет создавать с использованием такой схемы обмена алгоритмы, быстродействие которых может быть увеличено за счет уменьшения количества итераций.

Список литературы

1. *Feistel H. Cryptography and Computer Privacy // Scientific American. – 1973. – V. 228, N. 5. – P. 15–23.*
2. *Nechvatal J., Barket E., Bassham L., Burr W., Dworkin M., Foti J., Roback E. Report on the Development of the Advanced Encryption Standard (AES) // Computer Security Division; Information Technology Laboratory; NIST: Technology Administration; U.S. Department of Commerce. – 2000. – 116 p.*
3. *Шеннон К. Э. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: ИЛ, 1963. – С. 333–402.*
4. *Nakahara J. Jr., Vandewalle J., Prenceel B. Diffusion analysis of Feistel Networks (Extended version). – Belgium: Katholieke Universiteit Leuven, div. E.S.A.T. – SISTA/COSIC. – 18 p.*
5. *Самойленко Н.І., Уфимцева В.Б. Дифузійний аналіз мережі Фейстеля зі схемами обміну на основі матриць Фібоначчі // Наукові вісті Національного технічного університету «Київський політехнічний інститут». – 2002. - № 6 (26). – С. 146-152.*
6. Rukhin A., Soto J. at al. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications // NIST Special Publication 800 – 22. – 2001. – 154 p.

Рецензент: д-р техн. наук, проф. Н.И. Самойленко, Харьковский национальный университет городского хозяйства имени А.Н. Бекетова.

Авторы*: КАРПЕНКО Николай Юрьевич*
Харьковский национальный университет городского хазяйства им. А.Н. Бекетова, кандидат технических наук, доцент.
Раб. тел. – 707-31-45, E-mail – nictomkar@rambler.ru.
УФИМЦЕВА Виктория Борисовна
Харьковский национальный университет городского хазяйства им. А.Н. Бекетова, кандидат технических наук, доцент.
Раб. тел. – 707-31-45, E-mail – vika.uf@gmail.com.

Анализ показників перемішування у мережах Фейстеля

М.Ю. Карпенко, В.Б. Уфимцева

У статті зосереджено увагу на дослідженні процедур перестановок в симетричних шифри зі структурою мережі Фейстеля (СФ) з метою поліпшення показників перемішування по Шеннону. А саме, на можливостях поліпшення показників перемішування при використанні в перестановці декількох циклів і операцій додавання в фактор-кільці Z / (q). Проведено аналіз найбільш відповідний з точки зору дифузійного процесу структури – схеми Фейстеля і досліджена доцільність використання у схемі обміну (СО) симетричного шифру циклічних операцій додавання.

Ключевые слова: *симетричне шифрування, мережі Фейстеля, схеми обміну, дифузія.*

Analysis of Mixing in Networks Feistel

N.Y. Karpenko, V.B. Ufimtseva

The article focuses on a study of the procedures of permutations in symmetric ciphers with Feistel network structure (SF) to improve the performance of mixing the Shannon. Namely, the possibility of improving performance by stirring using a permutation several cycles and addition operations in the factor ring Z / (q). The analysis of the most suitable from the point of view of the diffusion process structure – Feistel scheme and investigate the feasibility of using a scheme of exchange (CO) symmetric cipher cycle operations of addition.

Keywords: *symmetrical encryption Feistel network, the circuit exchange, diffusion.*